CLAIMS

What is claimed is:

1. A method comprising:

receiving remotely originating data (ROD);

creating a customized identification (CID) which is at least partially created through encrypting the ROD as a function of a platform key (PK) and a random number (RN) of a computer system receiving the ROD;

receiving content including at least one watermark in which at least part of the CID is embedded; and

creating authentication comparison data (ACD) which is at least partially created through decrypting data embedded in the watermark.

2. The method of claim 1, wherein the ACD is created through decrypting CID in the content as a function of the PK and RN, and the ACD is compared with the ROD and the content is allowed to be played or not depending on an outcome of the comparison.

3. The method of claim 1, wherein the content includes first and second data sets, wherein the first data set is used to create a watermark key (WK) and the second data set is extracted utilizing the WK and the ACD includes at least part of the second data set.

4. The method of claim 3, wherein the first data set is relatively easy to extract from the content and the second data set is very difficult to extract without access to the first data set.

5. The method of claim 3, wherein the first data set includes the CID and RN and the second data set includes the ROD.

6. The method of claim 5, wherein the second data set further includes user or vender data.

7. The method of claim 3, wherein the first data set includes the ROD and RN and the second data set includes the CID.

8. The method of claim 7, wherein the second data set further includes user or vender data.

9. An apparatus comprising:

storage media including instructions stored thereon which when executed cause a computer system to perform a method including:

receiving remotely originating data (ROD);

creating a customized identification (CID) which is at least partially created through encrypting the ROD as a function of a platform key (PK) and a random number (RN) of a computer system receiving the ROD;

receiving content including at least one watermark in which at least part of the CID is embedded; and

creating authentication comparison data (ACD) which is at least partially created through decrypting data embedded in the watermark.

10. The apparatus of claim 9, wherein the ACD is created through decrypting CID in the content as a function of the PK and RN, and the ACD is compared with the ROD and the content is allowed to be played or not depending on an outcome of the comparison.

11. The apparatus of claim 10, wherein the content includes first and second data sets, wherein the first data set is used to create a watermark key (WK) and the second data set is extracted utilizing the WK and the ACD includes at least part of the second data set.

12. The apparatus of claim 11, wherein the first data set is relatively easy to extract from the content and the second data set is very difficult to extract without access to the first data set.

13. The apparatus method of claim 11, wherein the first data set includes the CID and RN and the second data set includes the ROD.

14. The apparatus method of claim 13, wherein the second data set further includes user or vender data.

15. The apparatus method of claim 11, wherein the first data set includes the ROD and RN and the second data set includes the CID.

16. The apparatus method of claim 15, wherein the second data set further includes user or vender data.

17. A method comprising:

providing data (RD) to be sent to a remote computer system;

receiving a customized identification (CID) which is a function of the RD and a platform key (PK) and a random number (RN) of a remote computer system;

providing content to be sent to a remote computer system, the content including at least one watermark in which at least part of the CID is embedded.

18. The method of claim 17, wherein the content includes first and second data sets, wherein the first data set is used to create a watermark key (WK) and the second data set may be extracted utilizing the WK and authentication comparison data (ACD), which is at least partially created through decrypting data embedded in the watermark.

19. The method of claim 18, wherein the first data set is relatively easy to extract from the content and the second data set is very difficult to extract without access to the first data set.

20. The method of claim 18, wherein the first data set includes the CID and RN and the second data set includes the ROD.

21. The method of claim 20, wherein the second data set further includes user or vender data.

22. The method of claim 18, wherein the first data set includes the ROD and RN and the second data set includes the CID.

23. The method of claim 22, wherein the second data set further includes user or vender data.

24. An apparatus comprising:

storage media including instructions stored thereon which when executed cause a computer system to perform a method including:

providing data (RD) to be sent to a remote computer system;

receiving a customized identification (CID) which is a function of the RD and a platform key (PK) and a random number (RN) of a remote computer system;

providing content to be sent to a remote computer system, the content including at least one watermark in which at least part of the CID is embedded.

25. The apparatus of claim 24, wherein the content includes first and second data sets, wherein the first data set is used to create a watermark key (WK) and the second data set may be extracted utilizing the WK and authentication comparison data (ACD), which is at least partially created through decrypting data embedded in the watermark.

26. The apparatus of claim 25, wherein the first data set is relatively easy to extract from the content and the second data set is very difficult to extract without access to the first data set.

27. The apparatus of claim 25, wherein the first data set includes the CID and RN and the second data set includes the ROD.

28. The apparatus of claim 27, wherein the second data set further includes user or vender data.

29. The apparatus of claim 25, wherein the first data set includes the ROD and RN and the second data set includes the CID.

30. The apparatus of claim 29, wherein the second data set further includes user or vender data.

31. A method comprising:

creating a customized identification (CID) which is at least partially created as a function of a platform key (PK); and

receiving content in which signals to control whether the content is played are embedded in the content and are knowable only to a system creating the CID, but wherein a content provider does not have access to a value of the PK.

32. The method of claim 31, wherein the content includes first and second data sets, wherein the first data set is used to create a watermark key (WK) and the second data set is extracted utilizing the WK.

33. The method of claim 32, wherein the first data set is relatively easy to extract from the content and the second data set is very difficult to extract without access to the first data set.